

REMARKS

Claims 2-7, 10-24, 27 and 30-32 are currently pending in the application. No changes have been made to the claims. Applicants wish to thank the Examiner for allowing claims 2-6, 10-24, 27 and 30-32.

The Examiner has rejected claim 7 as anticipated by U.S. patent no. 6,175,827 to Cordery et al. ('827). Applicants respectfully traverse this rejection.

The subject invention as claimed in claim 7 and the invention taught in the '827 patent are related only in that both seek to overcome problems which may be encountered in the use of encryption technology to verify an indicium or token, particularly an indicium or token used to evidence proper payment of postage for a mail piece. (For purposes of this response only the terms "indicium" and "token" are taken to be equivalent.) The problem addressed by the subject invention relates to certification of public keys, i.e. how to distribute public keys, and particularly the large number public keys used by postage meters of various mailers, so that an authority which uses a public key (which is putatively a key for a user authorized to generate indicia) to verify an indicium, can be sure that that key actually corresponds to the private key of the putative user. (Specification, pg. 1, line 21 - pg. 2 - line 16). In contrast, the '827 patent addresses the wholly separate problem of automatically verifying an indicium when the representation of that indicium has been degraded during scanning or other input to a verification system. ('827, col. 8, lines 18 - 32). These problems are clearly distinct and, as will be set forth more fully below, the present invention and the invention taught in the '827 patent can each be used either together with, or separately from, the other without change in either; so that there is no need or likelihood that the teaching of '827 will in any way suggest the invention of claim 7.

Claim 7 recites:

A article having an indicium imprinted thereon as evidence of attributes of said article, said indicium comprising:

a) a signature generated with a private key of a first party;

b) a certificate;

c) information specifying attributes of said article; wherein

d) said private key of said first party is generated as a function of said certificate, said information, and a private key of a certifying authority, said function being chosen so that a party wishing to verify said indicium can determine a public key corresponding to said private key of said first party by operating on said certificate and said information with a corresponding public key of said certifying authority.

Thus claim 7 claims an article having a printed indicium that serves as evidence of attributes of the article. The indicium includes a signature created with a private key of a first party, a certificate, and information specifying attributes of the article.

Subparagraph d) further limits the claimed invention by setting forth a relationship among these elements of the indicium such that a party wishing to verify the indicium can operate on the specifying information and the certificate with the public key of a certifying authority to generate the public key corresponding to the private key used to create the signature; thus in one step both obtaining and certifying as authentic the public key needed to verify the indicium.

In rejecting claim 7 as being anticipated, the Examiner, as he must, states that each limitation of the claim is taught by the '827 reference; particularly that the

limitation of subparagraph d) is taught by the '827 patent at col. 10, lines 21 - 60. Applicants respectfully submit that the Examiner has misinterpreted the teaching of '827.

What '827 teaches is that certain information (coordinates of the address block, numbers of lines, words, and characters in the address block, print font used, etc.) can be incorporated in the cyphertext and used together with an Error Correcting Code (ECC) to essentially eliminate errors in processing the address (col. 10, lines 9 - 26) and to deter and detect duplicate indicium. (Col. 10, lines 27 - 60). It will be readily apparent to those skilled in the art that this teaching is completely silent as to how the cyphertext is to be encrypted, much less as to how public keys corresponding to private keys used to encrypt the cyphertext can be certified and distributed.

Nor, in view of the repeated statements in '827 that the invention of '827 is independent of the encryption and certification techniques used, is it surprising that such teaching cannot be found anywhere in '827.

"For example if a public key cryptographic scheme is used, then the indicium can contain a digital signature (with or without public key certificate signed by a Certification Authority) as well as just cyphertext." (emphasis added) (col. 10, lines 5 -9).

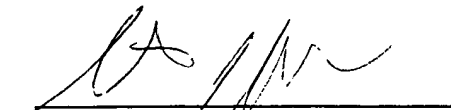
"It should be recognized that the particular printing system and the particular verifying system is a matter of systems design choice." (col. 12, lines 47 - 49).

"...the particular encryption algorithm employed may vary depending on the system design choice." (col. 15, lines 53 - 55).

In view of the above discussion, Applicants respectfully submit that the '827 patent neither teaches nor suggests, whether considered alone or in combination with other references cited but not applied, the invention of claim 7.

It is submitted that the application stands in condition for allowance. Reconsideration of the rejection is respectfully requested and an early notice of allowance earnestly solicited. If however, the Examiner has any questions please contact the undersigned at the number below.

Respectfully submitted,



Steven J. Shapiro
Reg. No. 35,677
Attorney of Record
Telephone (203) 924-3880

PITNEY BOWES INC.
Intellectual Property and
Technology Law Department
35 Waterview Drive
P.O. Box 3000
Shelton, CT 06484-8000